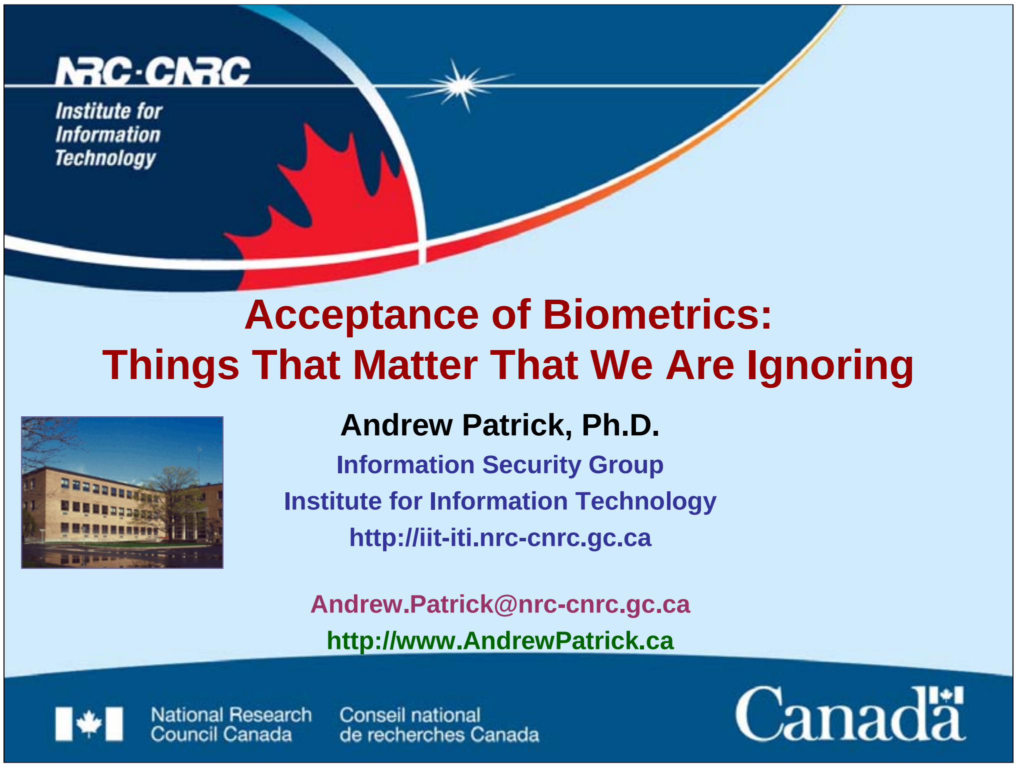


NRC·CNRC
Institute for Information Technology

Acceptance of Biometrics: Things That Matter That We Are Ignoring

Andrew Patrick, Ph.D.
Information Security Group
Institute for Information Technology
http://iit-iti.nrc-cnrc.gc.ca

Andrew.Patrick@nrc-cnrc.gc.ca
http://www.AndrewPatrick.ca

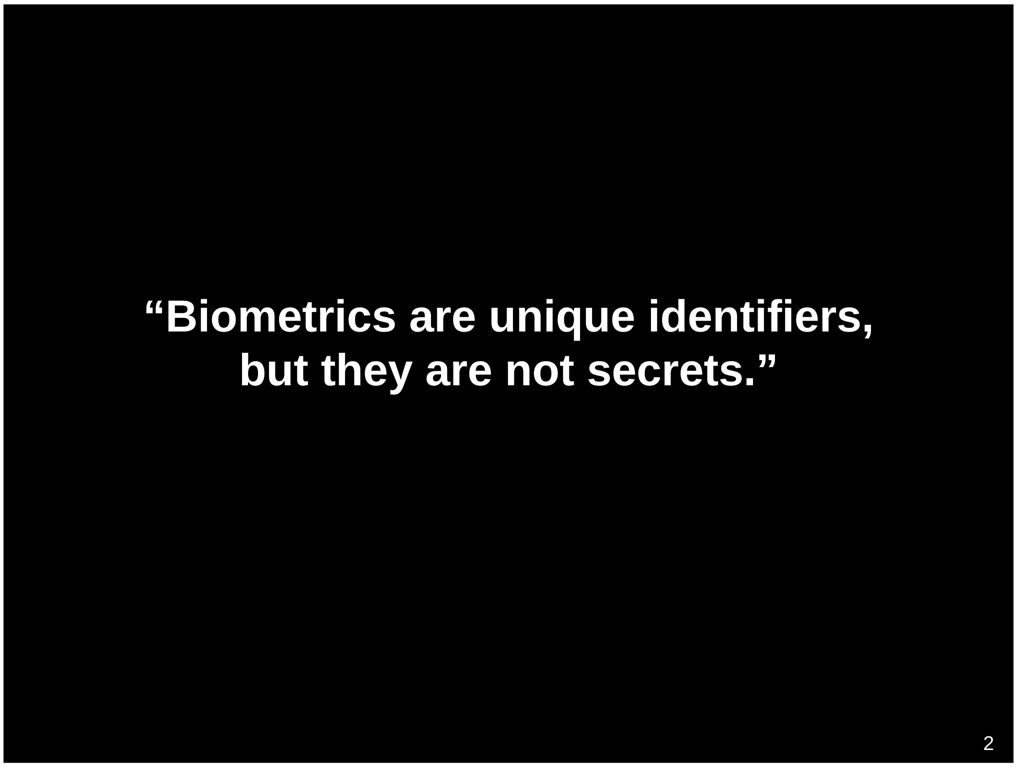
National Research Council Canada
Conseil national de recherches Canada
Canada

Presentation to the International Workshop on Usability and Biometrics, June 23-24, 2008, Washington, D.C.

Workshop organized by NIST and sponsored by DHS and US-VISIT.

For more information, see http://zing.ncsl.nist.gov/biousa/

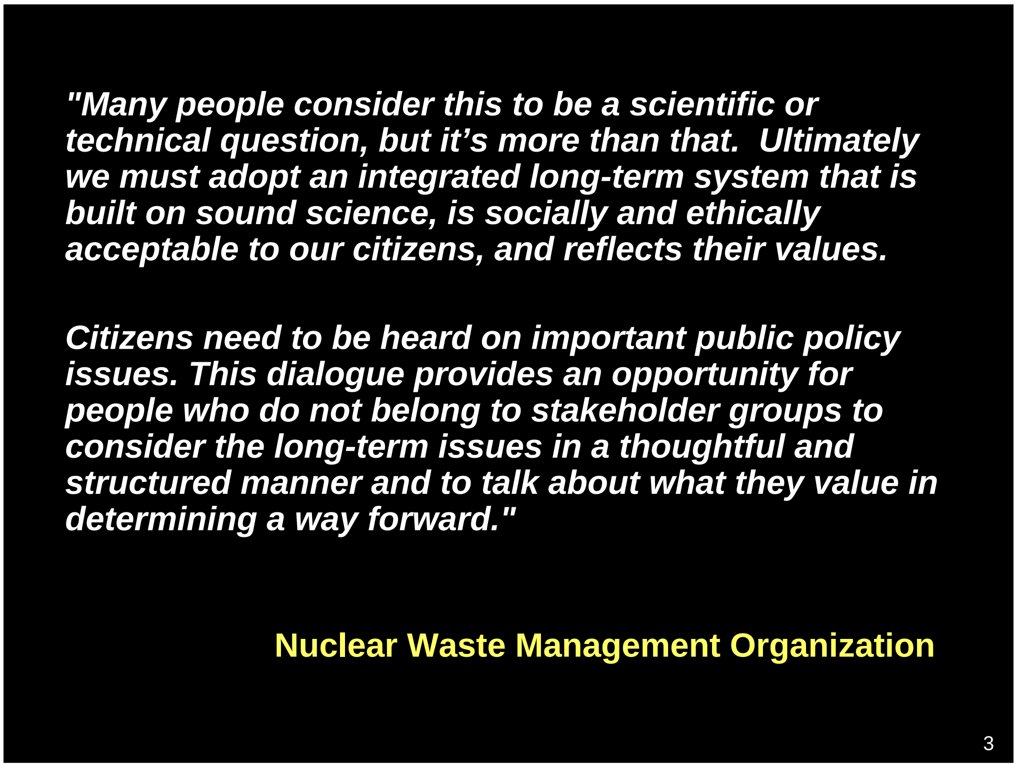
Dr. Andrew Patrick is a Senior Scientist at the National Research Council of Canada and an Adjunct Research Professor of Psychology at Carleton University. He is currently conducting research on new tools for privacy protection, the human factors of security systems, and trust decisions in e-commerce contexts. Prior to joining the NRC, Dr. Patrick worked at Nortel where he managed research and development groups focused on Voice over IP (VoIP) quality, and conducted field research to evaluated new product and service concepts. Dr. Patrick has also worked at the Communications Research Centre, where he conducted research on new multimedia services and natural language interfaces. WWW Site: www.andrewpatrick.ca



“Biometrics are unique identifiers, but they are not secrets.”

There is an elephant in the room, and this is the elephant…

This fundamental characteristic of biometrics should govern everything that we do, and we should not ignore it, but we often do. We can’t just accept it.



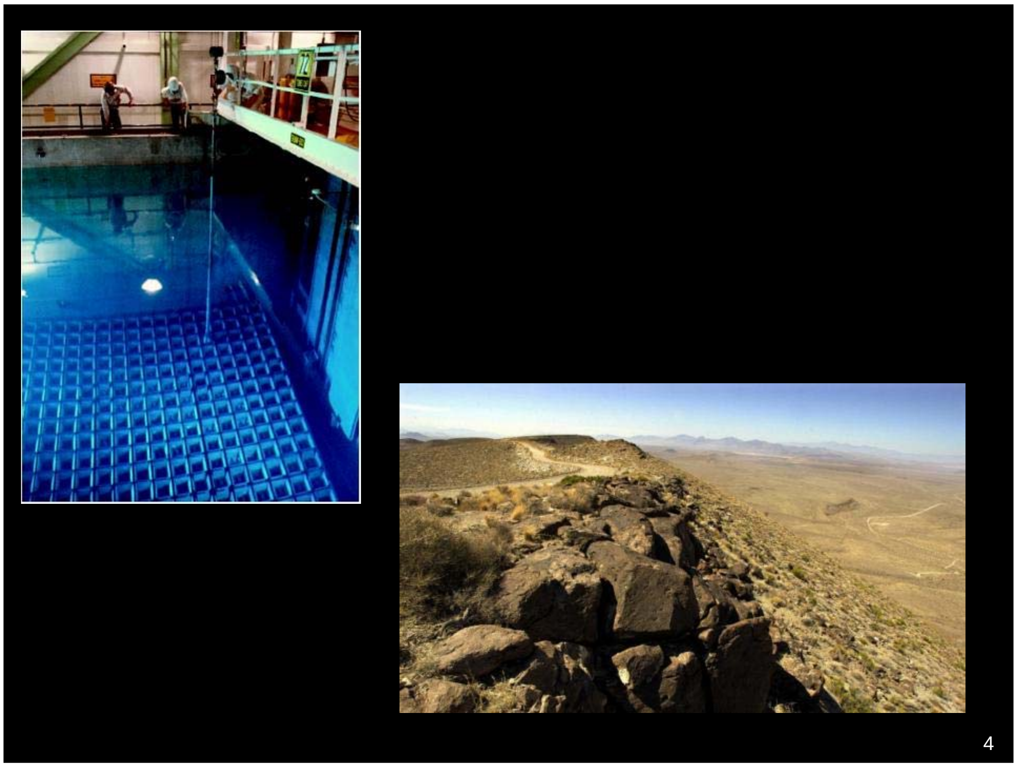
"Many people consider this to be a scientific or technical question, but it’s more than that. Ultimately we must adopt an integrated long-term system that is built on sound science, is socially and ethically acceptable to our citizens, and reflects their values.

Citizens need to be heard on important public policy issues. This dialogue provides an opportunity for people who do not belong to stakeholder groups to consider the long-term issues in a thoughtful and structured manner and to talk about what they value in determining a way forward."

Nuclear Waste Management Organization

This quotation might be a good description of the need for a socio-technical discussion about biometrics. It describes the need for a long-term strategy, a discussion of public policy, and consultation with stakeholders.

This quote is not about biometrics, however, but is instead about nuclear waste…



I want to argue that there is a strong parallel between biometrics and nuclear power. Both biometrics and nuclear power have very attractive properties – they promise attractive solutions to long-term problems. And yet they both have fundamental problems that have not been addressed, privacy for biometrics and nuclear waste for nuclear power. And the problems get harder and harder to solve the longer they are left unaddressed. Initially, the solution for nuclear waste was storage within the power facilities… a long-term solution was left for later, and coming up with a long-term solution now is proving very difficult (witness the heated debates about the proposed Yucca Mountain Repository).

The fundamental problems about biometrics may seem esoteric and far-off now, but as the technology and economics changes, so will the risks and attacks. Copying biometric information from the environment (e.g., harvesting latent fingerprints), spoofing, hacking, reconstructing biometric information from templates, insider attacks, and theft of body parts may all seem far-fetched now, but they could become common if the use of biometrics becomes widespread and the value of the information protected by biometrics increases.

Consider Internet-based fraud. Initially it was a collection of esoteric attacks without any large-scale threats or benefits. As more and more people started using the Internet for financial transactions, however, the benefits of conducting fraud on the Internet grew and the types of attacks become widespread and effective. Today we are faced with a large collection of attacks, including phishing, pharming, Trojan horses, man-in-the-middle attacks, and good old fashion confidence tricks. The root problem is the unsecure nature of the Internet, and not addressing this problem early on has allowed all of these threats to flourish. Let's not make the same mistake about biometrics.

Photo Credits:

http://graphics.boston.com/resize/bonzai-fba/Globe_Photo/2007/12/02/1196654189_5005/539w.jpg

http://www.pollutionissues.com/Pl-Re/Radioactive-Waste.html

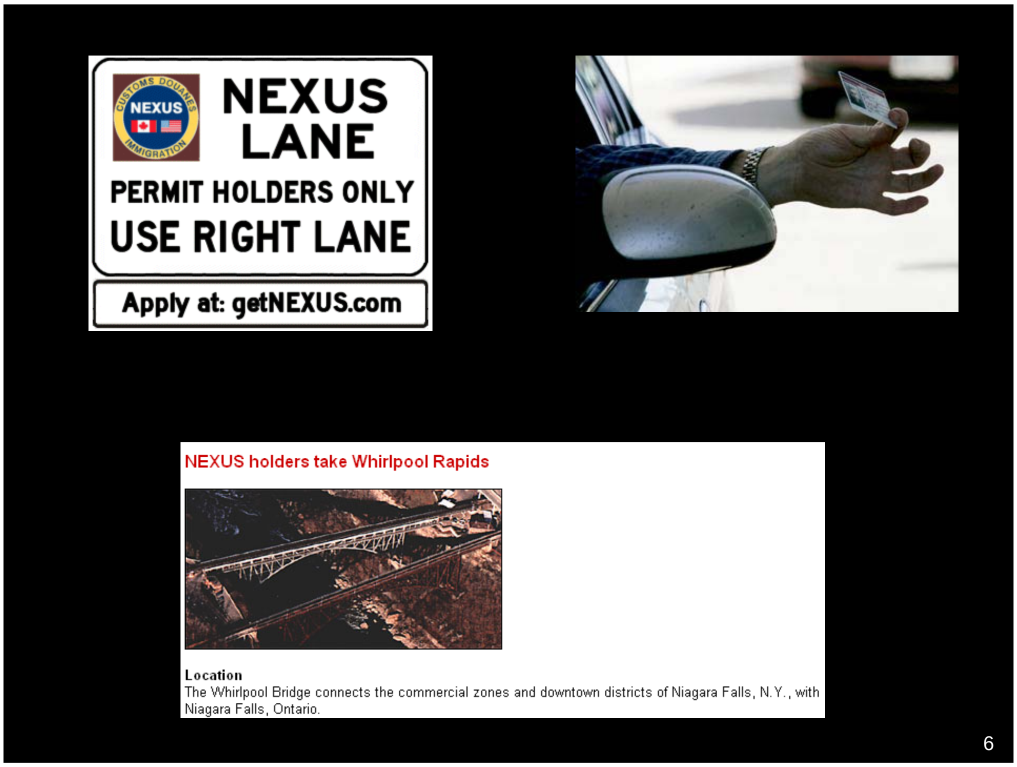
policy matters

5

We will return to the elephant later, but first let’s consider other things that matter, other things that we should not be ignoring.

Policy matters.

Policies affect daily lives, and we usually have to live with policy decisions for a long time.



NEXUS holders take Whirlpool Rapids

Location
The Whirlpool Bridge connects the commercial zones and downtown districts of Niagara Falls, N.Y., with Niagara Falls, Ontario.

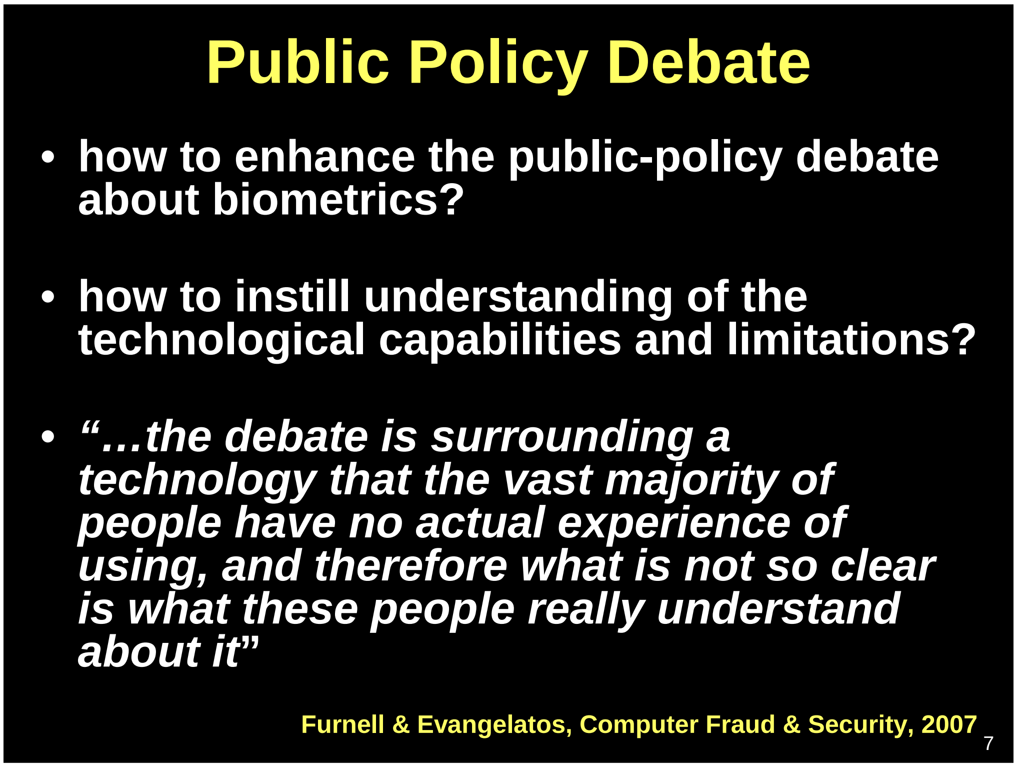
6

Consider one example. I grew up in Niagara Falls, where one quickly learned how to avoid the thousands of tourists who visit there. I had a large extended family that lived and worked on both sides of the US-Canada border, so learning how to cross the border while avoiding tourists was important. The solution was a little-known Whirlpool Bridge, and ancient steel bridge that had decks for cars and trains and connected the two downtown areas.

Recently, use of the bridge has been restricted to NEXUS subscribers, a frequent traveler program that requires people to submit their fingerprints during the application process, and their iris and face images if they are accepted.

Although participation in the NEXUS program is described as “completely voluntary”, for my family this policy decision forces them to either get NEXUS or don’t visit with the extended family. Supposed “voluntary” systems may not actually be voluntary.

Policy matters.



Public Policy Debate

- how to enhance the public-policy debate about biometrics?
- how to instill understanding of the technological capabilities and limitations?
- *"…the debate is surrounding a technology that the vast majority of people have no actual experience of using, and therefore what is not so clear is what these people really understand about it"*

Furnell & Evangelatos, Computer Fraud & Security, 2007

7

There needs to be an informed public-policy debate about biometrics. There needs to be clear discussions about the capabilities and limitations of biometric systems. We need to discuss when they should be deployed, and where they should be avoided.

This debate is difficult, especially since policy makers are often asked to talk about things that they have no experience with and no deep understanding.

As usability professionals, it is important that we get involved in the public policy debate. We have to move beyond usability as rhetoric and start using our knowledge of people and technology to build better systems.

Usability is more than the placement of fingers on readers or the proper height for iris cameras. It is about the entire spectrum on human-technology interaction, and it is important to ask "why" in addition to "how."

context matters

8

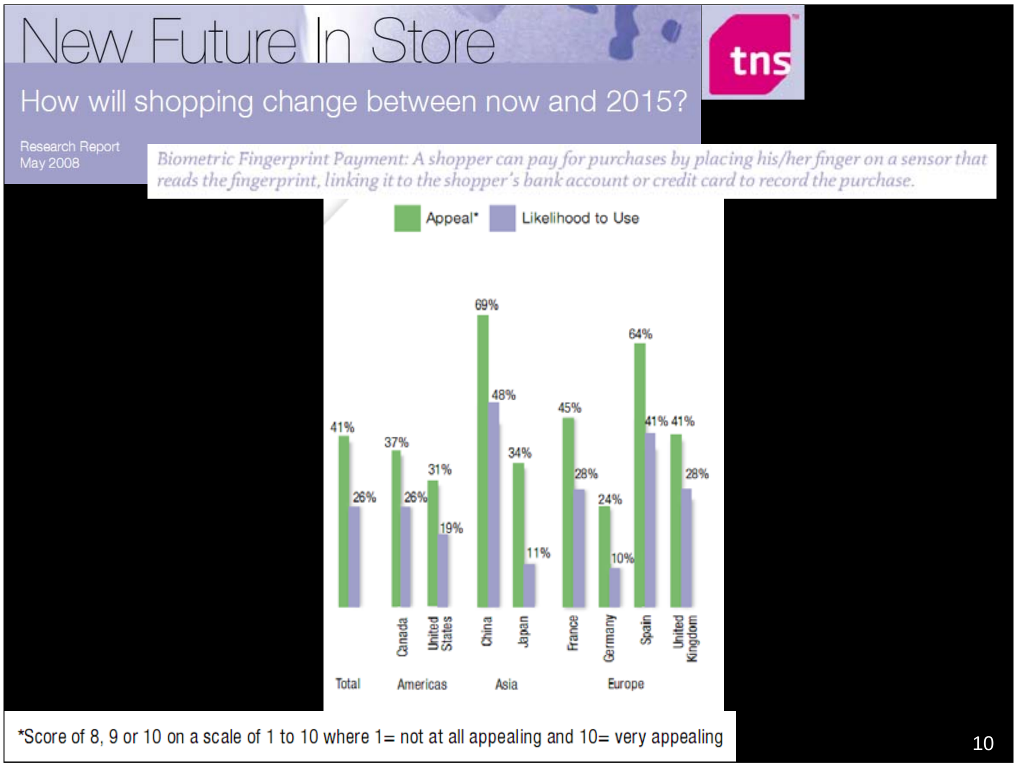
Context refers to the identity, place, time, and activity that is associated with using a biometric system.

Context matters.

For example, the acceptance of biometrics in a commercial context will likely be quite different from acceptance for border control or other government applications.

Biometric systems are showing up in a wide variety of contexts, meaning places, applications, authorities, importance, etc.

To most people, the biometrics systems may appear to be the same (e.g., a fingerprint reader that they touch), but the functions and purposes of the system can be very different. They are confused when they are asked to use a biometric for a convenience application (login to a laptop or pay for milk and bread), while the same biometric is used for a national security application (border crossing).



New Future In Store

How will shopping change between now and 2015?

Research Report
May 2008

Biometric Fingerprint Payment: A shopper can pay for purchases by placing his/her finger on a sensor that reads the fingerprint, linking it to the shopper's bank account or credit card to record the purchase.

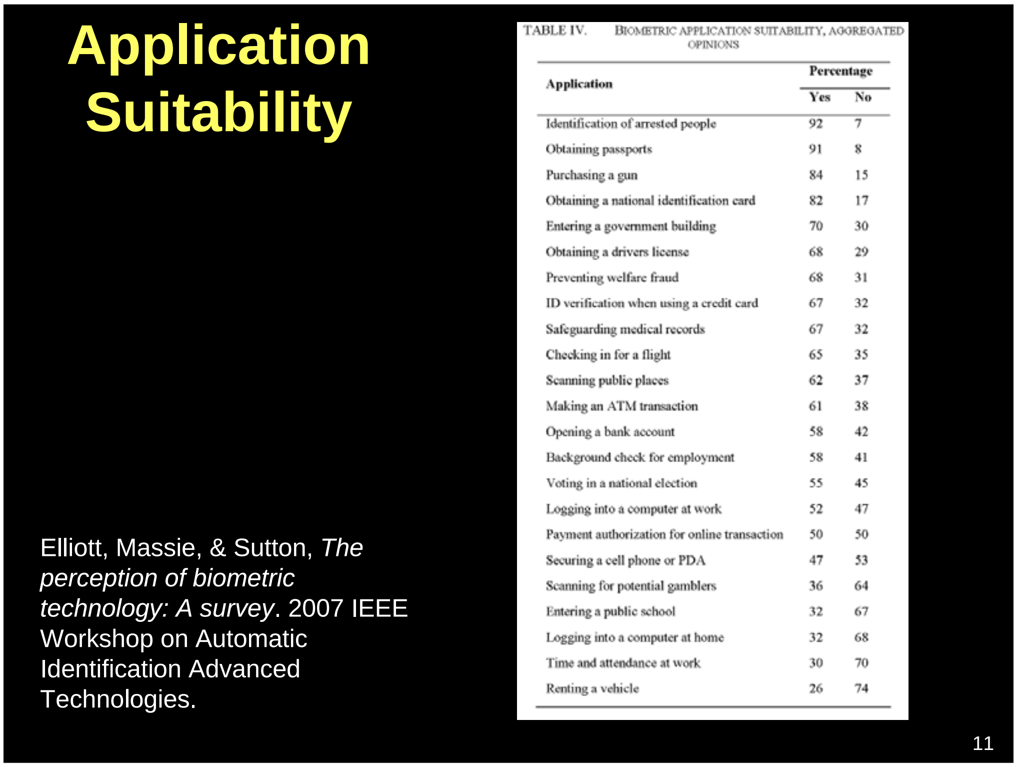
*Score of 8, 9 or 10 on a scale of 1 to 10 where 1= not at all appealing and 10= very appealing

Context also matters on a large scale. This recent report looked at attitudes towards using biometrics to pay for goods when shopping. This chart shows that the attitudes differ a great deal around the world, with the most positive attitudes in Asia, and the least positive in the Americas.

Source.

"New Future in Store" Report for www.tnsglobal.com

4,600 online surveys with primary household shoppers during Jan-Feb 2008



Application Suitability

TABLE IV. BIOMETRIC APPLICATION SUITABILITY, AGGREGATED OPINIONS

Application	Percentage	
	Yes	No
Identification of arrested people	92	7
Obtaining passports	91	8
Purchasing a gun	84	15
Obtaining a national identification card	82	17
Entering a government building	70	30
Obtaining a drivers license	68	29
Preventing welfare fraud	68	31
ID verification when using a credit card	67	32
Safeguarding medical records	67	32
Checking in for a flight	65	35
Scanning public places	62	37
Making an ATM transaction	61	38
Opening a bank account	58	42
Background check for employment	58	41
Voting in a national election	55	45
Logging into a computer at work	52	47
Payment authorization for online transaction	50	50
Securing a cell phone or PDA	47	53
Scanning for potential gamblers	36	64
Entering a public school	32	67
Logging into a computer at home	32	68
Time and attendance at work	30	70
Renting a vehicle	26	74

Elliott, Massie, & Sutton, *The perception of biometric technology: A survey*. 2007 IEEE Workshop on Automatic Identification Advanced Technologies.

11

Context also refers to the purpose of using biometrics. This tables show the percentage of people who think that biometrics are suitable for different applications. Clearly, opinions about suitability differ depending on the application.

Context matters.

Concerns are often not with the biometric system, but with the back-end processes and policies

12

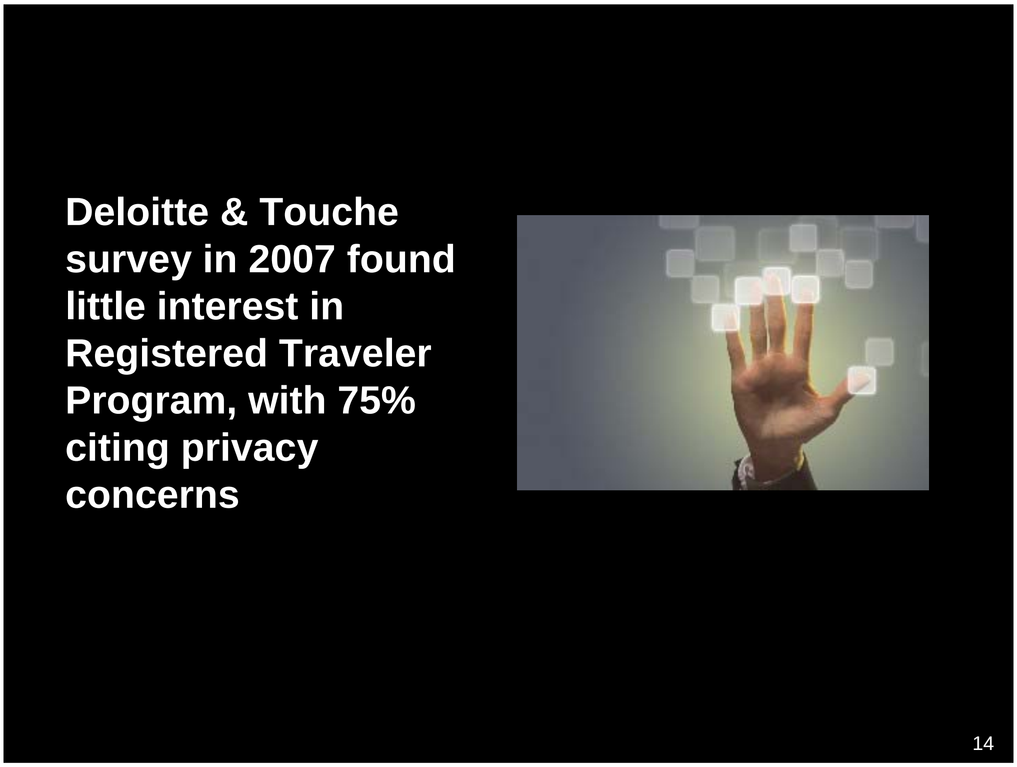
Biometrics are also used in a context of larger information and security systems. Biometric systems involve much more than gathering physical or behavioral characteristics. Research findings often show that peoples' concerns about biometrics are not with the measurement of human characteristics, but with the associated systems, processes, and polices.

Context matters.

privacy matters

Let’s return to the elephant. Privacy matters for biometrics.

In many places, use of biometrics is governed by privacy laws and regulations. More and more regulators are requiring detailed privacy assessments before systems can be put in place. And in some places, such as Canada, regulators are putting strict requirements on such systems, such as requiring encryption, ensuring single use, no match to latents, strict access controls, separate storage of personal information, etc.



Deloitte & Touche survey in 2007 found little interest in Registered Traveler Program, with 75% citing privacy concerns

Privacy matters for acceptance. There is evidence that people consider privacy when deciding whether to enroll in “voluntary” services, such as frequent traveler programs.

Source:

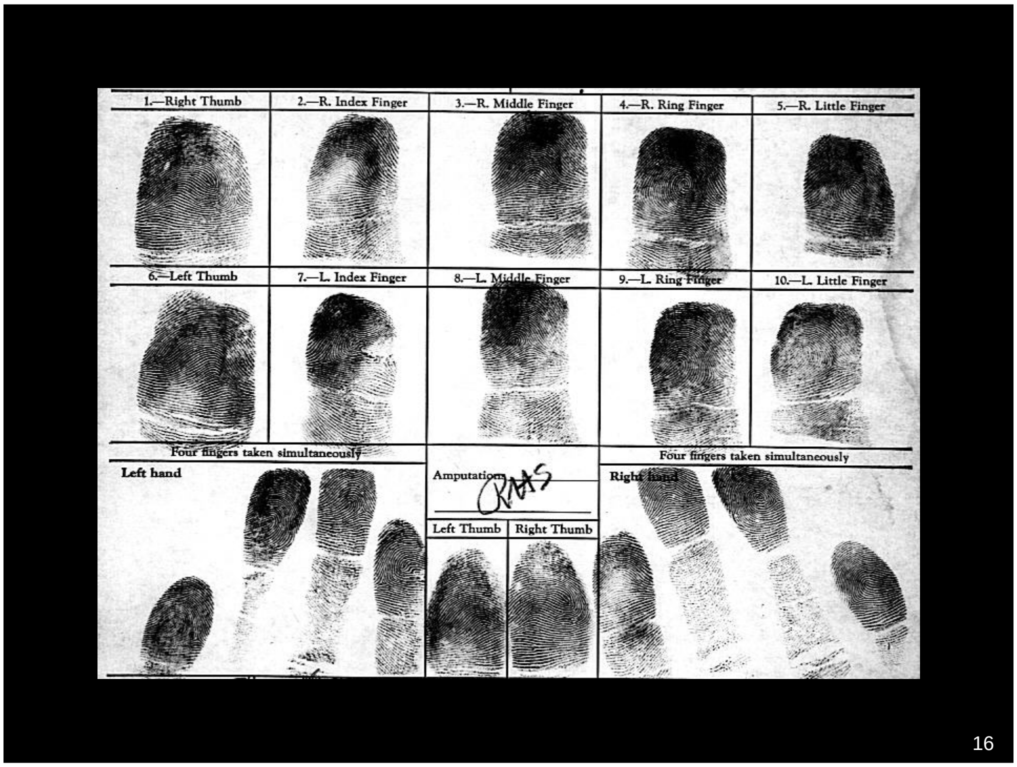
http://sev.prnewswire.com/travel/20070404/NYW03304042007-1.html

Basteltips Biometrieversand
Das biometrische Sammelalbum
Otto Schily
Ex-Innenminister
Jörg Ziercke
BKA-Präsident
die datenschleuder. #92 / 2008
15

As a protest against his support for the increasing use of biometric data, the influential hacker group Chaos Computer Club published one of Wolfgang Schäuble's fingerprints in the March 2008 edition of its magazine Datenschleuder (Schäuble is the federal Minister of the Interior). The magazine also included the print on a film that readers could use to fool fingerprint readers.

They did this by collecting a latent fingerprint, because (remember the elephant) biometrics are not secret.

Why did this story get so much attention if this is a fundamental characteristic of biometrics? Why are adopters of biometric systems ignoring the non-secret nature of biometrics?

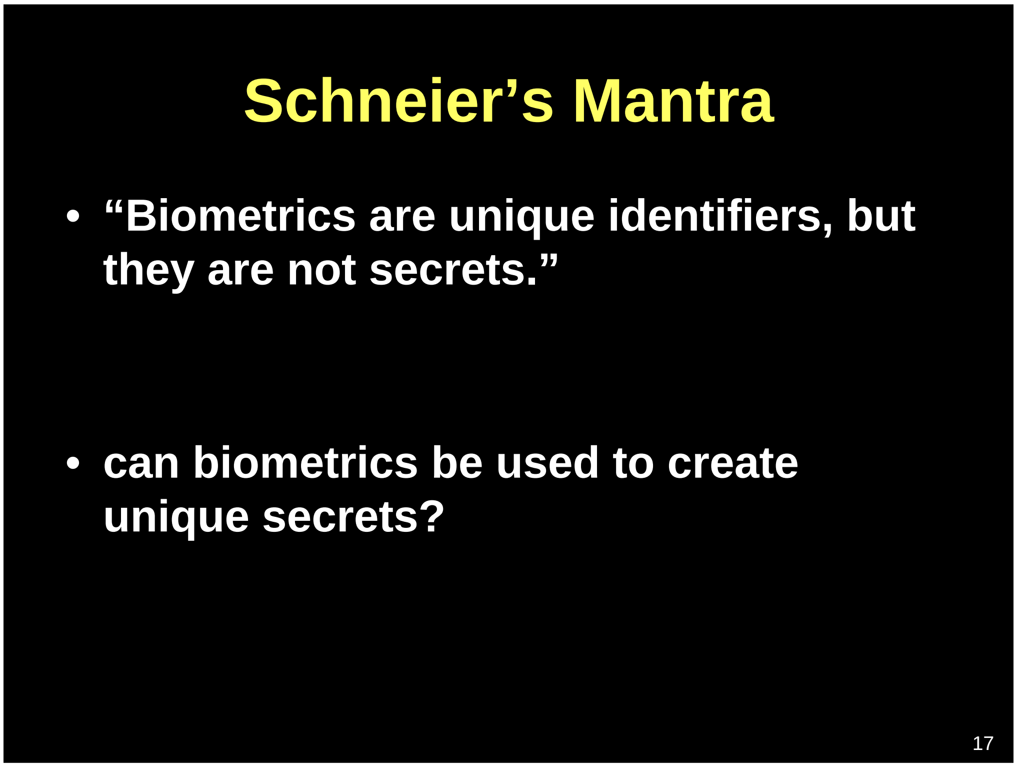


Pretend that these are my fingerprints. They have been published on the Internet and downloaded over 1000 times.

Does this give me plausible deniability? Could I argue, if my fingerprints were ever found somewhere, there it is plausible that they were spoofed using information freely available to anyone on the Internet. There have been cases of fraudulent planting of latent prints, does my publishing of my prints mean that latent matching is useless for me?

Does this make my fingerprints of less value to the US-Visit program? Robert Mocny, the Director of US-VISIT, said during his keynote address to this workshop that users of biometrics systems must be careful because "even one breach of the data will undermine all our systems." (May not be an exact quote.) But the information is not secret in the first place!

Further, Mr. Mocny also described a proposal to have travel carriers (airlines, shipping companies) collect biometrics for the exit portion of the US-VISIT program (currently, biometrics are only collected when visitors enter the U.S.). Does shifting the responsibility for biometric collection to third parties (who do not have the motivation to do this well) not increase the risk of data breaches?



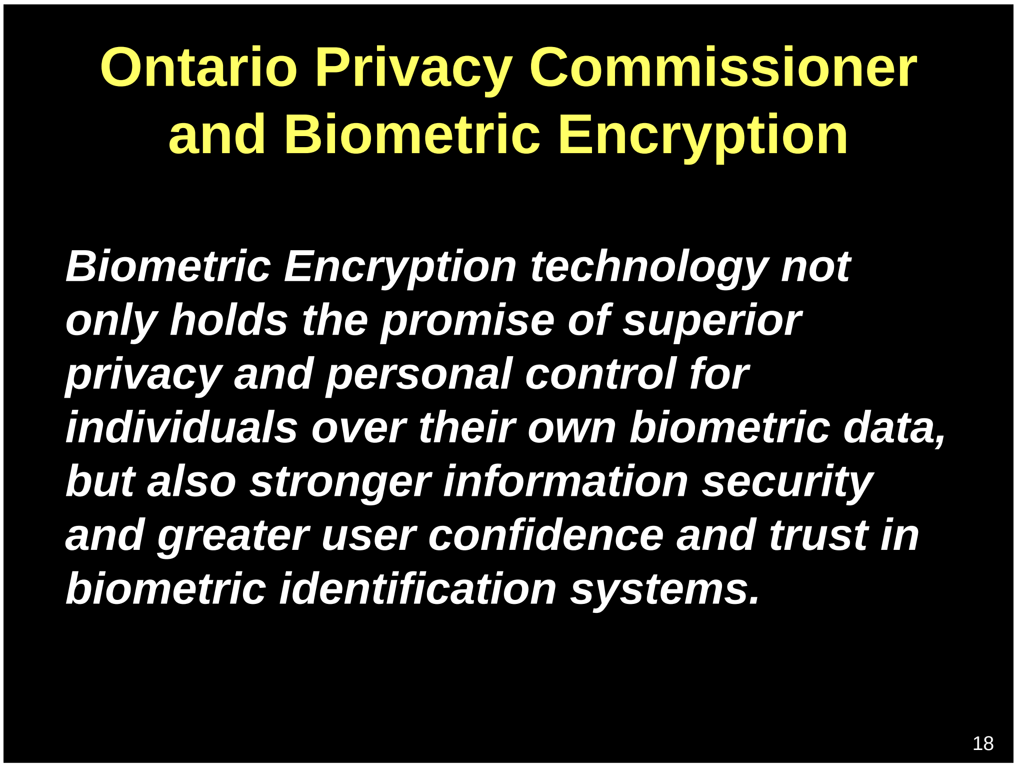
Schneier’s Mantra

- “Biometrics are unique identifiers, but they are not secrets.”
- can biometrics be used to create unique secrets?

17

Bruce Schneier is the person responsible for the elephant statement.

One possible response to the challenge that biometrics are not secrets is to find a way to make them into secrets, or to use them to create unique secrets…



Ontario Privacy Commissioner and Biometric Encryption

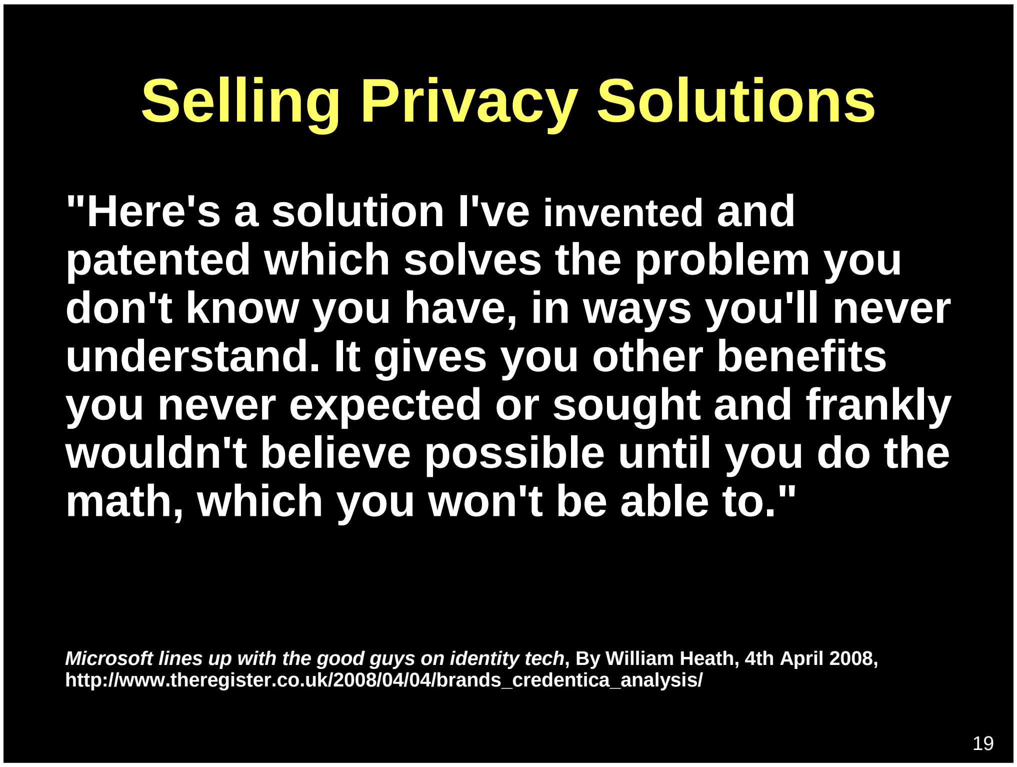
Biometric Encryption technology not only holds the promise of superior privacy and personal control for individuals over their own biometric data, but also stronger information security and greater user confidence and trust in biometric identification systems.

18

This is an area that we should be exploring. For example, in Ontario the Privacy Commissioner has recently released a white paper describing her interest in biometric encryption as a tool for doing reliable identification while protecting privacy.

Further, the Commissioner has involved in a number of projects where biometric encryption is being tried in different deployment contexts.

This is important work when trying to manage the elephant.



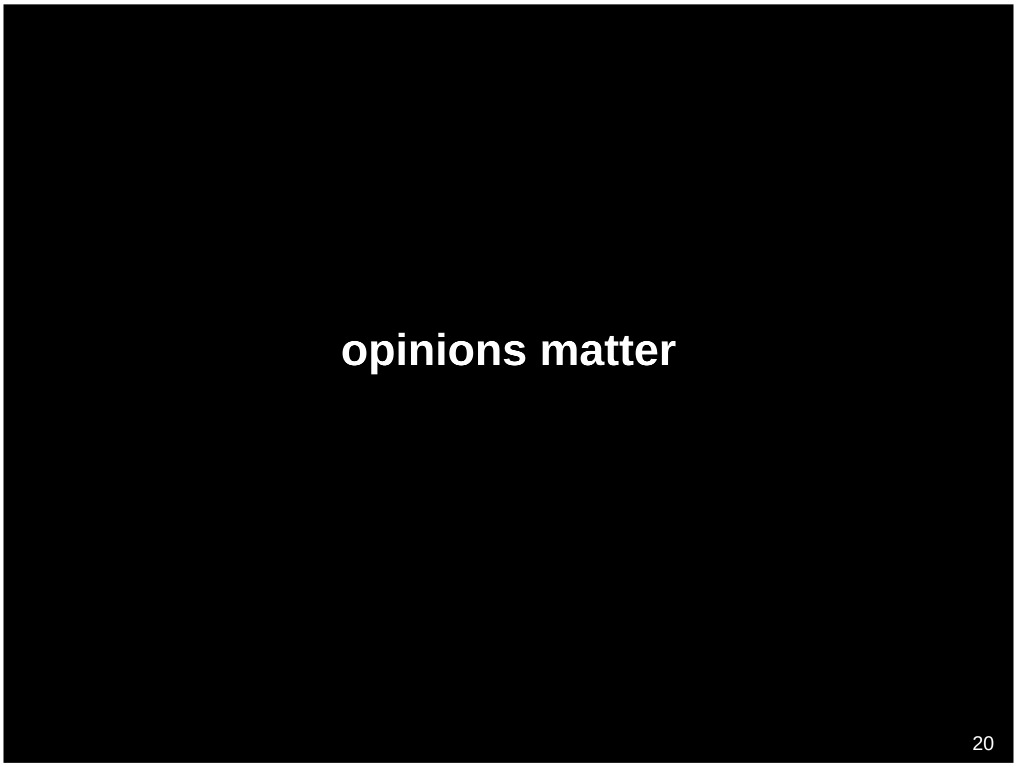
Selling Privacy Solutions

"Here's a solution I've invented and patented which solves the problem you don't know you have, in ways you'll never understand. It gives you other benefits you never expected or sought and frankly wouldn't believe possible until you do the math, which you won't be able to."

Microsoft lines up with the good guys on identity tech, By William Heath, 4th April 2008, http://www.theregister.co.uk/2008/04/04/brands_credentica_analysis/

Addressing the privacy problem inherent in biometrics is not easy. This quote describes the nature of privacy problems and solutions, and it applies well to biometric systems.

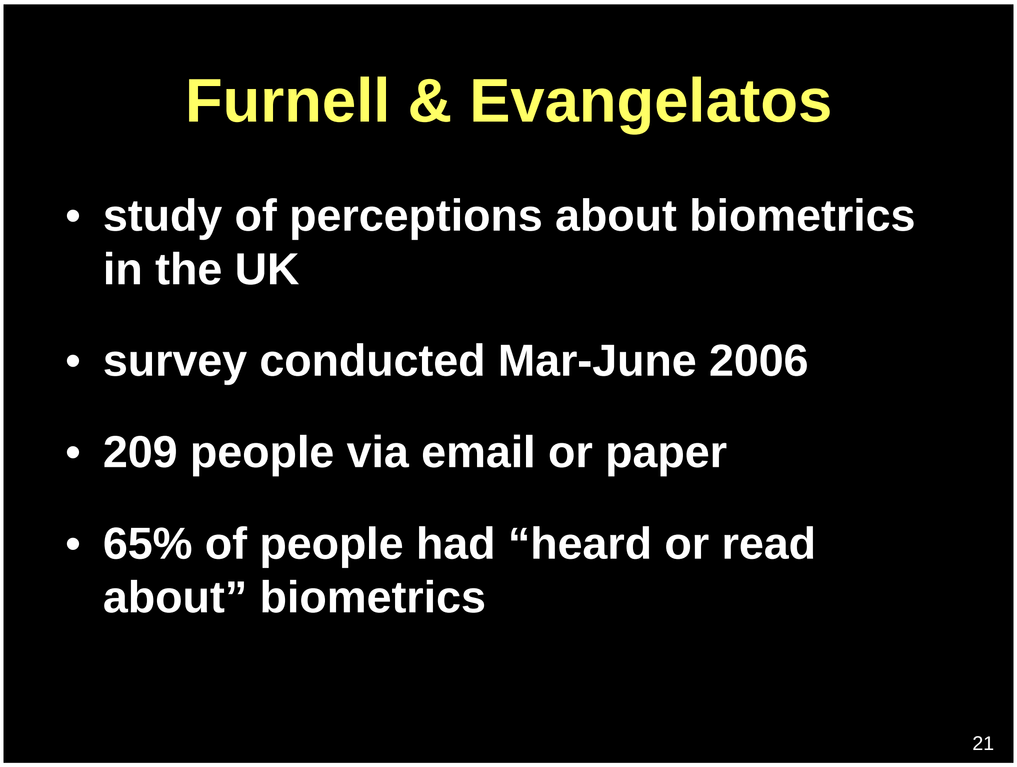
And yet we can’t be scared away. Enhancing the privacy of biometric systems is fundamental.



opinions matter

Another thing that matters is public opinion. Even in cases where people are forced to use biometric systems, such as mandatory national ID schemes, opinions matter.

We know, for example, that people who understand and value a biometric system will be more compliant when using it, and will produce higher quality biometric information (e.g., better fingerprint images).

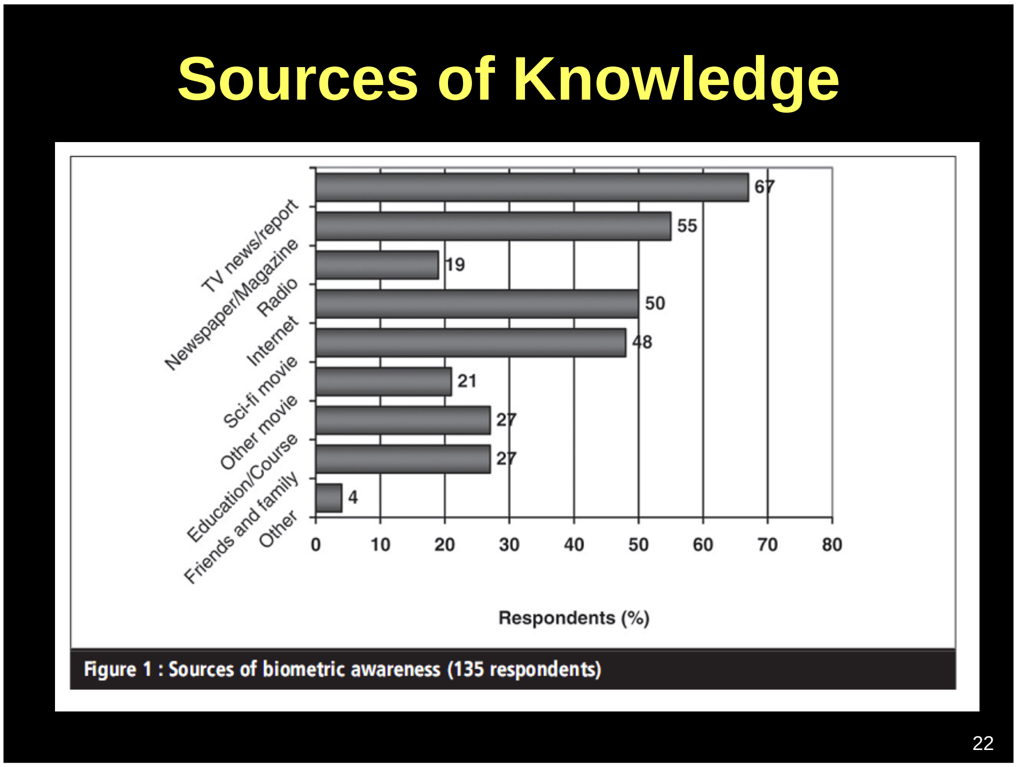


Furnell & Evangelatos

- study of perceptions about biometrics in the UK
- survey conducted Mar-June 2006
- 209 people via email or paper
- 65% of people had “heard or read about” biometrics

Consider one recent study of opinions of biometrics. This study is not unique, but is instead typical of research on opinions in this area.

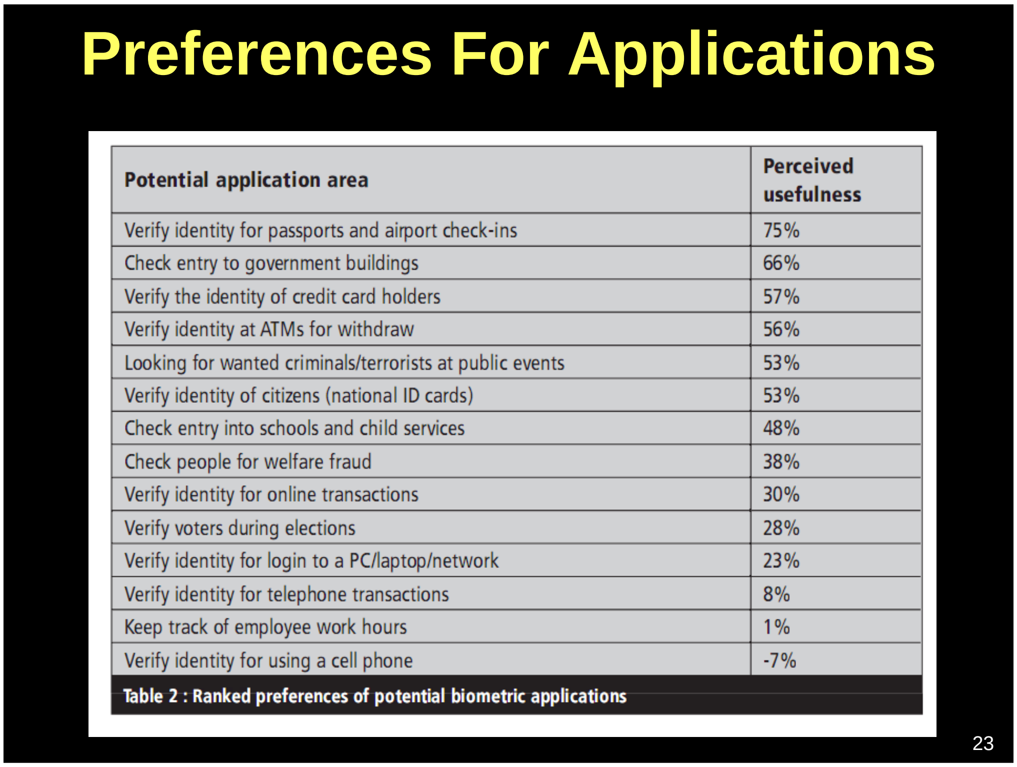
Contrary to what policy makers may claim, public opinions about biometrics are not generally positive, and people have serious concerns and a fundamental lack of understanding.



Sources of Knowledge

Figure 1 : Sources of biometric awareness (135 respondents)

Note the frequency of non-factual sources, such as sci-fi movies, and perhaps the Internet.

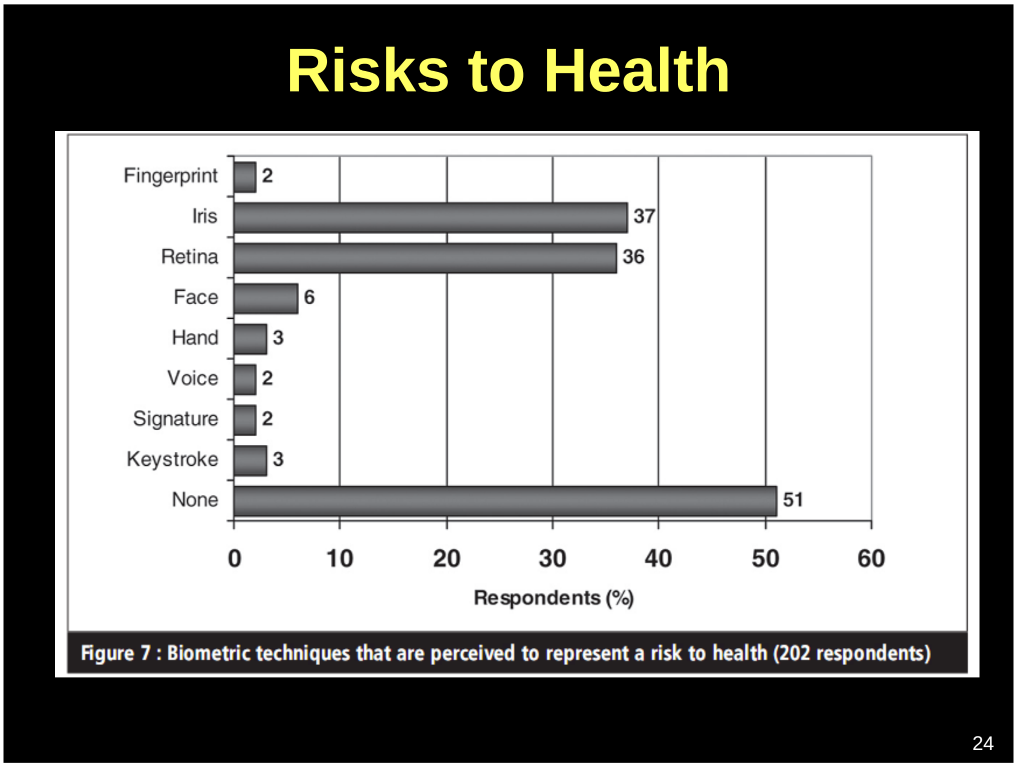


Preferences For Applications

Potential application area	Perceived usefulness
Verify identity for passports and airport check-ins	75%
Check entry to government buildings	66%
Verify the identity of credit card holders	57%
Verify identity at ATMs for withdraw	56%
Looking for wanted criminals/terrorists at public events	53%
Verify identity of citizens (national ID cards)	53%
Check entry into schools and child services	48%
Check people for welfare fraud	38%
Verify identity for online transactions	30%
Verify voters during elections	28%
Verify identity for login to a PC/laptop/network	23%
Verify identity for telephone transactions	8%
Keep track of employee work hours	1%
Verify identity for using a cell phone	-7%

Table 2 : Ranked preferences of potential biometric applications

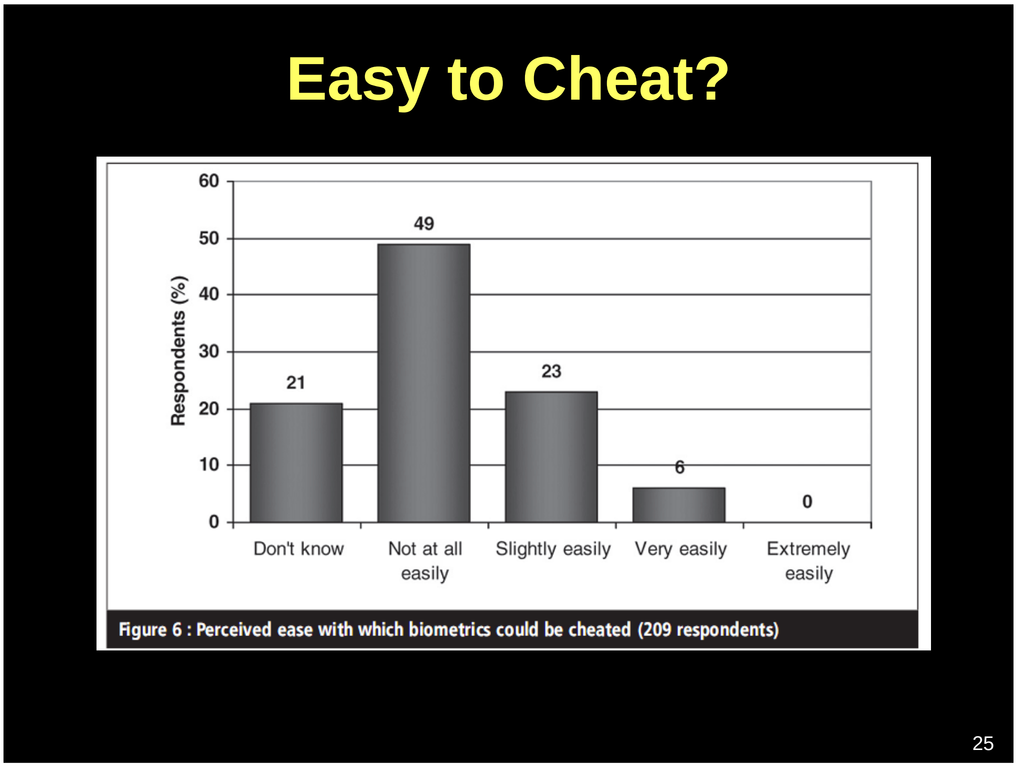
Again, context matters when people think about different applications for biometrics. Using biometrics in passports is considered to be far more useful than using them for monitoring work hours.



Risks to Health

Figure 7 : Biometric techniques that are perceived to represent a risk to health (202 respondents)

People have opinions about health risks that may not represent the actual risks. People are particularly concerned about biometrics that involved the eye, and my observations are that people often do not know the difference between the iris and retina, nor how biometrics systems use these characteristics.



Easy to Cheat?

Figure 6 : Perceived ease with which biometrics could be cheated (209 respondents)

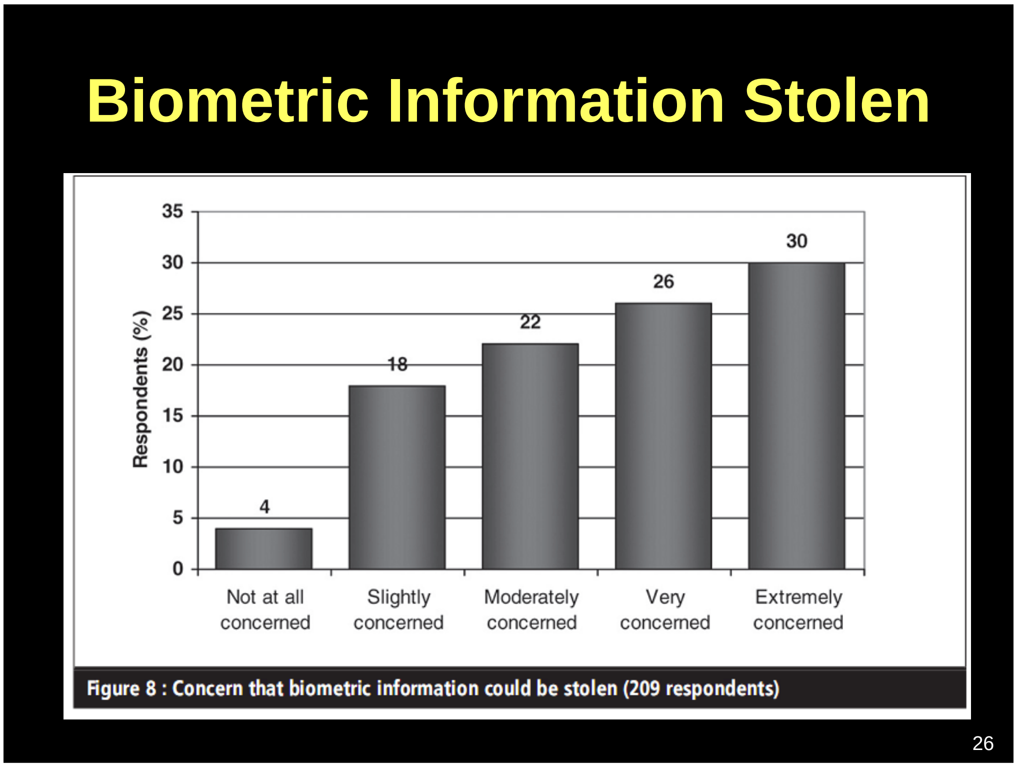
25

People are fairly confident that biometrics are not easy to cheat, although this confidence my be misplaced.

Robert Mocny, the Director of US-VISIT, described a desire to have biometric systems be as easy to use as ATM machines, where people can withdraw money in local currency throughout the world. This is a terrible goal.

Although ATM machines might be easy to use, they are also easy to attack. Many forms of ATM-based fraud are common, including card skimming and cloning. Criminals have successfully attacked ATM networks and back-end servers. And insiders have used secret information to conduct fraud.

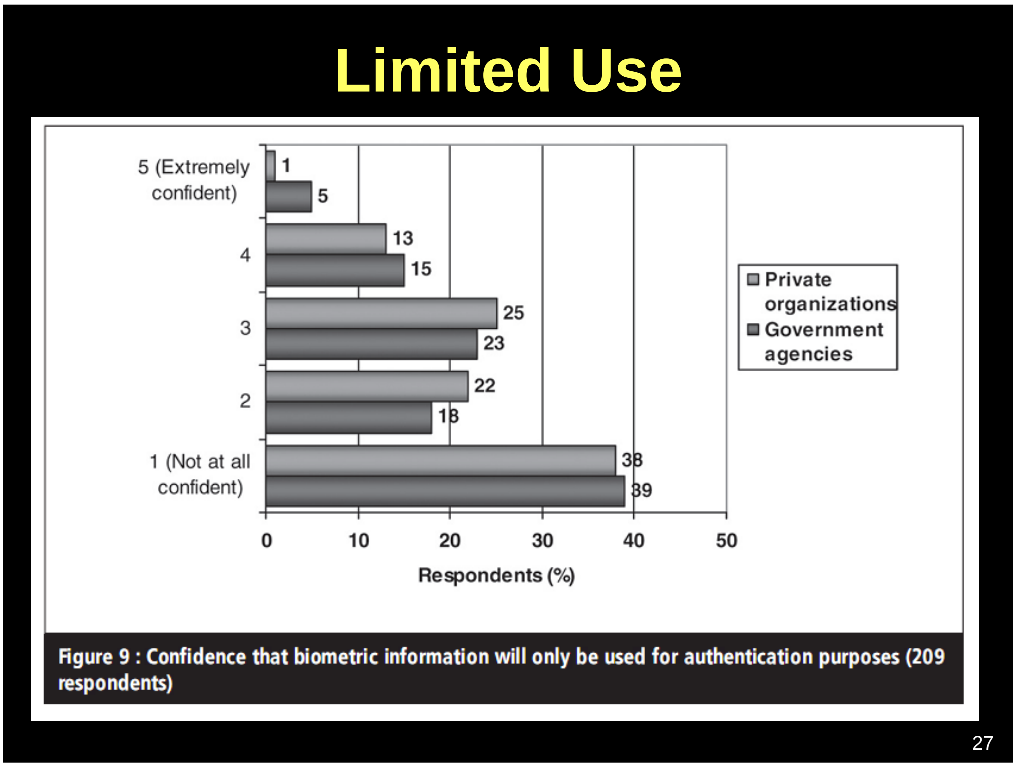
When building biometric systems, we must build things that are far more secure than ATM machines.



Biometric Information Stolen

Figure 8 : Concern that biometric information could be stolen (209 respondents)

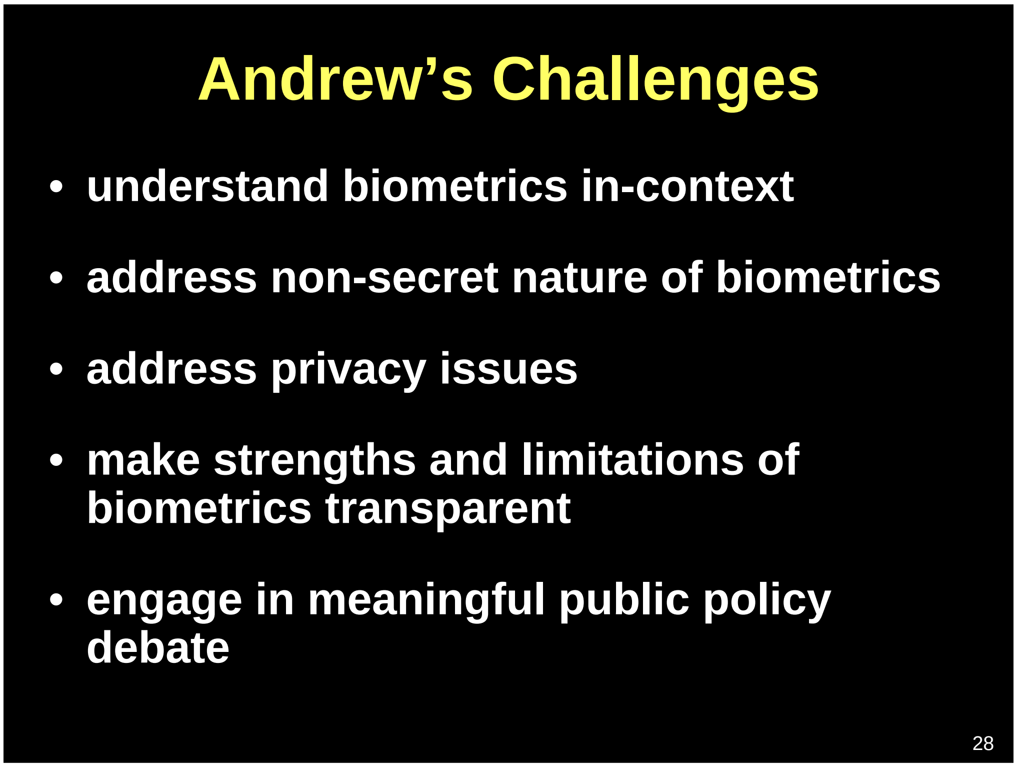
People are very concerned that their biometric information could be stolen…



Limited Use

Figure 9 : Confidence that biometric information will only be used for authentication purposes (209 respondents)

… and they are not confident that organizations will limit their use of biometric information, especially governments.



Andrew’s Challenges

- understand biometrics in-context
- address non-secret nature of biometrics
- address privacy issues
- make strengths and limitations of biometrics transparent
- engage in meaningful public policy debate

To summarize, these are key challenges that we have to address. These things matter, and we should not continue to ignore them as we rush to introduce more and more biometric systems.